Amendments to the Claims

The listing of claims below will replace all prior versions and listings of claims in the application.

1. (Previously Presented) An e-mail method, comprising:

recognizing that an unauthorized electronic mail message is about to be sent from a computing device configured to send an electronic mail message; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

2. (Previously Presented) The method as recited in claim 1, wherein said recognizing that an unauthorized electronic mail message is about to be sent comprises detecting that a send function has been initiated by an unauthorized agent.

3. (Previously Presented) The method as recited in claim 2, wherein the unauthorized agent is a virus.

4. (Previously Presented) The method as recited in claim 1, further comprising stopping transmission of the unauthorized electronic mail message in response to the instruction input via the user interface.

5. (Previously Presented) The method as recited in claim 1, further comprising deleting the unauthorized electronic mail message, prior to transmission of the unauthorized electronic mail message, in response to the instruction input via the user interface.

6. (Previously Presented) An e-mail method, comprising:

recognizing that an unauthorized electronic mail message is about to be sent from a computing device configured to send an electronic mail message;

displaying at least information relating to an addressee of the unauthorized electronic mail message in a user interface configured to receive as input an instruction to stop transmission of the unauthorized electronic mail message; and

stopping transmission of the unauthorized electronic mail message in response to the instruction input via the user interface.

7. (Previously Presented) An e-mail method, comprising:

recognizing that an unauthorized electronic mail message is about to be sent from a computing device configured to send an electronic mail message;

displaying at least information relating to an addressee of the unauthorized electronic mail message in a user interface configured to receive as input an instruction to delete the unauthorized electronic mail message; and

deleting the unauthorized electronic mail message, prior to transmission of the unauthorized electronic mail message, in response to the instruction input via the user interface.

8. (Previously Presented) The method as recited in claim 1, further comprising displaying the unauthorized electronic mail message, and wherein the user interface is configured to receive as input an instruction to modify the unauthorized electronic mail message, cancel transmission of the unauthorized electronic mail message, or authorize transmission of the unauthorized electronic mail message.

9. (Previously Presented) An apparatus, comprising:

a computing device configured to:

send an e-mail message;

recognize that an unauthorized e-mail message is about to be sent from the computing device; and

control a send operation of the unauthorized e-mail message from the computing device responsive to recognizing that the unauthorized e-mail message is about to be sent from the computing device, said control including providing an alert, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized e-mail message.

10. (Previously Presented) An article of manufacture including a computer readable storage medium having stored thereon computer executable instructions, execution of which by a computing device causes the computing device to perform operations comprising:

recognizing that an unauthorized electronic mail message is about to be sent from the computing device; and

controlling a send operation of the unauthorized electronic mail message responsive

to recognizing that the unauthorized electronic mail message is about to be sent from the computing device, said controlling a send operation including providing an alert, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

11. (Previously Presented) An electronic mail message alert display, comprising:

a text display configured to provide an alert indicating that an unauthorized electronic mail message is about to be sent from a computing device and to display at least information relating to an addressee of the unauthorized electronic mail message; and

a user interface configured to receive as input ~~of~~ an instruction to stop transmission of the unauthorized electronic mail message.

12. (Previously Presented) An e-mail method, comprising:

determining that an unauthorized electronic mail message composed by a virus is about to be sent from a computing device configured to send an electronic mail message; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

13. (Previously Presented) An e-mail method, comprising:

determining that an unauthorized electronic mail message about to be sent from a computing device configured to send an electronic mail message is being sent by an

unauthorized agent; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

Claims 14 - 22. (Cancelled)

23. (Previously Presented) An e-mail method, comprising:

recognizing that an unauthorized electronic mail message composed by a process configured to compose an unauthorized electronic mail message is about to be sent from a computing device configured to send an electronic mail message; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

24. (Previously Presented) The method as recited in claim 23, wherein the process is a virus.

25. (Previously Presented) The method as recited in claim 23, wherein the process is an unauthorized agent.

26. (Previously Presented) An e-mail method, comprising:

recognizing that an electronic mail message about to be sent from a computing device configured to send an electronic mail message is an unauthorized electronic mail message; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

27. (Previously Presented) An article of manufacture including a computer readable storage medium having stored thereon computer executable instructions, execution of which by a computing device causes the computing device to perform operations comprising:

recognizing that an electronic mail message about to be sent from a computing device configured to send an electronic mail message is an unauthorized electronic mail message; and

providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

28. (Cancelled)

29. (Previously Presented) An e-mail system, comprising:

means for recognizing that an unauthorized electronic mail message is about to be sent from a computing device configured to send an electronic mail message; and

means for providing at the computing device an alert indicating that the unauthorized electronic mail message is about to be sent, the alert being provided by a user interface configured to receive as input an instruction for further processing of the unauthorized electronic mail message.

30. (Previously Presented) The method of claim 1, wherein the unauthorized electronic mail is composed by a virus and has a valid recipient address.

31. (Previously Presented) The method of claim 1, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

32. (Previously Presented) The method of claim 6, wherein the unauthorized electronic mail is composed by a virus and has a valid recipient address.

33. (Previously Presented) The method of claim 6, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

34. (Previously Presented) The method of claim 7, wherein the unauthorized electronic mail message is composed by a virus and has a valid recipient address.

35. (Previously Presented) The method of claim 7, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

36. (Previously Presented) The apparatus of claim 9, wherein the unauthorized e-mail message is composed by a virus and has a valid recipient address.

37. (Previously Presented) The apparatus of claim 9, wherein the computing device is configured to detect that a send operation has been initiated and recognize that the unauthorized e-mail message is about to be sent.

38. (Previously Presented) The article of manufacture of claim 10, wherein the operations further comprise recognizing the unauthorized electronic mail message is composed by a virus and has a valid recipient address.

39. (Previously Presented) The article of manufacture of claim 10, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

40. (Previously Presented) The display of claim 11, wherein the text display indicates the unauthorized electronic mail message is composed by a virus and has a valid recipient address.

41. (Previously Presented) The method of claim 23, wherein the unauthorized electronic mail message has a valid recipient address.

42. (Previously Presented) The method of claim 23, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

43. (Previously Presented) The method of claim 26, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

44. (Previously Presented) The article of manufacture of claim 27, wherein said recognizing that an unauthorized electronic mail message is about to be sent includes detecting that a send operation has been initiated.

45. (Previously Presented) The system of claim 29, wherein said means for recognizing that an unauthorized electronic mail message is about to be sent includes means for detecting that a send operation has been initiated.

46. (Cancelled).

47. (Previously Presented) The apparatus of claim 9, wherein said computing device is configured to control the send operation by stopping transmission of the unauthorized e-mail message, in response to the instruction input via the user interface.

48. (Previously Presented) The apparatus of claim 9, wherein said computing device is configured to control the send operation by deleting the unauthorized e-mail message, prior to transmission of the unauthorized e-mail message, in response to the instruction input via the user interface.

49. (Currently Amended) The ~~apparatus~~system of claim 29, further comprising:

means for stopping transmission of the unauthorized electronic mail message in response to the instruction input via the user interface.

50. (Currently Amended) The ~~apparatus~~system of claim 29, further comprising:

means for deleting the unauthorized electronic mail message, prior to transmission of the unauthorized electronic mail message, in response to the instruction input via the user interface.

51. (Cancelled).

52. (Previously Presented) The article of manufacture of claim 10, wherein said controlling a send operation of the unauthorized electronic mail message includes stopping transmission of the unauthorized electronic mail message in response to the instruction input via the user interface.

53. (Previously Presented) The article of manufacture of claim 10, wherein said controlling a send operation of the unauthorized electronic mail message includes deleting the unauthorized electronic mail message, prior to transmission of the unauthorized electronic mail message, in response to the instruction input via the user interface.

54. (Previously Presented) The method as recited in claim 1, further comprising modifying the addressee of the unauthorized electronic mail message in response to the instruction input via the user interface.

55. (Previously Presented) The method as recited in claim 1, further comprising modifying a text of the unauthorized electronic mail message in response to the instruction input via the user interface.

56. (Previously Presented) The method as recited in claim 1, further comprising displaying at least a list of plural addressees of the unauthorized electronic mail message in the user interface, wherein the user interface is configured to receive as input an instruction to modify an addressee in the list of plural addressees.